95TH CONGRESS } HOUSE OF REPRESENTATIVES { REPORT
2d Session } { No. 95-1720

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

OCTOBER 5, 1978.—Ordered to be printed

Mr. BOLAND, from the committee of conference, submitted the following

CONFERENCE REPORT

[To accompany S. 1566]

The committee of conference on the disagreeing votes of the two Houses on the amendments of the House to the bill (S. 1566) to authorize electronic surveillance to obtain foreign intelligence information, having met, after full and free conference, have agreed to recommend and do recommend to their respective Houses as follows:

That the Senate recede from its disagreement to the amendment of the House to the text of the Senate bill, and agree to the same with an amendment as follows:

In lieu of the matter proposed to be inserted by the House amendments insert the following:

That this Act may be cited as the "Foreign Intelligence Surveillance Act of 1978".

TABLE OF CONTENTS

TITLE I—ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

DEFINITIONS

SEC. 101. As used in this title:

(a) "Foreign power" means—

(1) a foreign government or any component thereof, whether or not recognized by the United States;

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons; or

(6) an entity that is directed and controlled by a foreign government or governments.

(b) "Agent of a foreign power" means—

(1) any person other than a United States person, who—

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a) (4);

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

(2) any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power; or

(D) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

(c) "*International terrorism*" means activities that—

(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any States;

(2) appear to be intended—

(A) to intimidate or coerce a civilian population;

(B) to influence the policy of a government by intimidation or coercion; or

(C) to affect the conduct of a government by assassination or kidnapping; and

(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

(d) "*Sabotage*" means activities that involve a violation of chapter 105 of title 18, United States Code, or that would involve such a violation if committed against the United States.

(e) "*Foreign intelligence informations*" means—

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage or international terrorism by a foreign power or an agent of a foreign power;

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

(f) "*Electronic surveillance*" means—

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

(g) "Attorney General" means the Attorney General of the United States (or Acting Attorney General) or the Deputy Attorney General.

(h) "Minimization procedures", with respect to electronic surveillance, means—

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1), shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 102(a), procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than twenty-four hours unless a court order under section 105 is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

(i) "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens law-

fully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a) (1), (2), or (3).

(j) "United States", when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

(k) "Aggrieved person" means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.

(l) "Wire communication" means any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.

(m) "Person" means any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power.

(n) "Contents", when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

(o) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Trust Territory of the Pacific Islands, and any territory or possession of the United States.

AUTHORIZATION FOR ELECTRONIC SURVEILLANCE FOR FOREIGN INTELLIGENCE PURPOSES

SEC. 102. (a)(1) Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that—

(A) the electronic surveillance is solely directed at—

(i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 101(a) (1), (2), or (3); or

(ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 101(a) (1), (2), or (3);

(B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and

(C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 101(h); and

if the Attorney General reports such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least

thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately.

(2) An electronic surveillance authorized by this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures adopted by him. The Attorney General shall assess compliance with such procedures and shall report such assessments to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence under the provisions of section 108(a).

(3) The Attorney General shall immediately transmit under seal to the court established under section 103(a) a copy of his certification. Such certification shall be maintained under security measures established by the Chief Justice with the concurrence of the Attorney General, in consultation with the Director of Central Intelligence, and shall remain sealed unless—

(A) an application for a court order with respect to the surveillance is made under sections 101(h)(4) and 104; or

(B) the certification is necessary to determine the legality of the surveillance under section 106(f).

(4) With respect to electronic surveillance authorized by this subsection, the Attorney General may direct a specified communication common carrier to—

(A) furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers; and

(B) maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished which such carrier wishes to retain.

The Government shall compensate, at the prevailing rate, such carrier for furnishing such aid.

(b) Applications for a court order under this title are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the court having jurisdiction under section 103, and a judge to whom an application is made may, notwithstanding any other law, grant an order, in conformity with section 105, approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information, except that the court shall not have jurisdiction to grant any order approving electronic surveillance directed solely as described in paragraph (1)(A) of subsection (a) unless such surveillance may involve the acquisition of communications of any United States person.

DESIGNATION OF JUDGES

SEC. 103. (a) The Chief Justice of the United States shall publicly designate seven district court judges from seven of the United States judicial circuits who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic

surveillance anywhere within the United States under the procedures set forth in this Act, except that no judge designated under this subsection shall hear the same application for electronic surveillance under this Act which has been denied previously by another judge designated under this subsection. If any judge so designated denies an application for an order authorizing electronic surveillance under this Act, such judge shall provide immediately for the record a written statement of each reason for his decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established in subsection (b).

(b) The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a court of review which shall have jurisdiction to review the denial of any application made under this Act. If such court determines that the application was properly denied, the court shall immediately provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

"(c) Proceedings under this Act shall be conducted as expeditiously as possible. The record of proceedings under this Act, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of Central Intelligence.

"(d) Each judge designated under this section shall so serve for a maximum of seven years and shall not be eligible for redesignation, except that the judges first designated under subsection (a) shall be designated for terms of from one to seven years so that one term expires each year, and that judges first designated under subsection (b) shall be designated for terms of three, five, and seven years.

APPLICATION FOR AN ORDER

SEC. 104. (a) Each application for an order approving electronic surveillance under this title shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 103. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this title. It shall include—

(1) the identity of the Federal officer making the application;

(2) the authority conferred on the Attorney General by the President of the United States and the approval of the Attorney General to make the application;

(3) the identity, if known, or a description of the target of the electronic surveillance;

(4) a statement of the facts and circumstances relied upon the applicant to justify his belief that—

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(5) a statement of the proposed minimization procedures;

(6) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;

(7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate—

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that the purpose of the surveillance is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 101(e); and

(E) including a statement of the basis for the certification that—

(i) the information sought is the type of foreign intelligence information designated; and

(ii) such information cannot reasonably be obtained by normal investigative techniques;

(8) a statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;

(9) a statement of the facts concerning all previous applications that have been made to any judge under this title involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application;

(10) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this title should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter; and

(11) whenever more than one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device.

(b) Whenever the target of the electronic surveillance is a foreign power, as defined in section 101(a) (1), (2), or (3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the application need not contain the information required by paragraphs (6), (7)(E), (8), (11) of subsection (a), but shall state whether physical entry is re-

quired to effect the surveillance and shall contain such information about the surveillance techniques and communications or other information concerning United States persons likely to be obtained as may be necessary to assess the proposed minimization procedures.

(c) The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

(d) The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 105.

ISSUANCE OF AN ORDER

SEC. 105. (a) Upon an application made pursuant to section 104, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that—

(1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;

(2) the application has been made by a Federal officer and approved by the Attorney General;

(3) on the basis of the facts submitted by the applicant there is probable cause to believe that—

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(4) the proposed minimization procedures meet the definition of minimization procedures under section 101(h); and

(5) the application which has been filed contains all statements and certifications required by section 104 and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 104(a)(7)(E) and any other information furnished under section 104(d).

(b) An order approving an electronic surveillance under this section shall—

(1) specify—

(A) the identity, if known, or a description of the target of the electronic surveillance;

(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed;

(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance;

(E) the period of time during which the electronic surveillance is approved; and

(F) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the devices involved and what minimization procedures shall apply to information subject to acquisition by each device; and

(2) direct—

(A) that the minimization procedures be followed;

(B) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minium of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;

(C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and

(D) that the applicant compensate at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.

(c) Whenever the target of the electronic surveillance is a foreign power, as defined in section 101(a) (1), (2), or (3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the order need not contain the information required by subparagraphs (C), (D), and (F) of subsection (b)(1), but shall generally describe the information sought, the communications or activities to be subjected to the surveillance, and the type of electronic surveillance involved, including whether physical entry is required.

(d)(1) An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose, or for ninety days, whichever is less, except that an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 101(a) (1), (2), or (3), for the period specified in the application or for one year, whichever is less.

(2) Extensions of an order issued under this title may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order, except that an extension of an order under this Act for a surveillance targeted against a foreign power, as defined in section 101 (a)(5) or (6), or against a foreign power as defined in section 101(a)(4) that is not a United States person, may be for a period not to exceed one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period.

(3) At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the

circumstances under which information concerning United States persons was acquired, retained, or disseminated.

(e) Notwithstanding any other provision of this title, when the Attorney General reasonably determines that—

(1) an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained; and

(2) the factual basis for issuance of an order under this title to approve such surveillance exists;

he may authorize the emergency employment of electronic surveillance if a judge having jurisdiction under section 103 is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to employ emergency electronic surveillance and if an application in accordance with this title is made to that judge as soon as practicable, but not more than twenty-four hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes such emergency employment of electronic surveillance, he shall require that the minimization procedures required by this title for the issuance of a judicial order be followed. In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of twenty-four hours from the time of authorization by the Attorney General, whichever is earliest. In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person. A denial of the application made under this subsection may be reviewed as provided in section 103.

(f) Notwithstanding any other provision of this title, officers, employees, or agents of the United States are authorized in the normal course of their official duties to conduct electronic surveillance not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to—

(1) test the capability of electronic equipment, if—

(A) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;

(B) the test is limited in extent and duration to that necessary to determine the capability of the equipment;

(C) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test per-

sonnel, and are destroyed before or immediately upon completion of the test; and:

(D) Provided, That the test may exceed ninety days only with the prior approval of the Attorney General;

(2) determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, if—

(A) it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and

(C) any information acquired by such surveillance is used only to enforce chapter 119 of title 18, United States Code, or section 605 of the Communications Act of 1934, or to protect information from unauthorized surveillance; or

(3) train intelligence personnel in the use of electronic surveillance equipment, if—

(A) it is not reasonable to—

(i) obtain the consent of the persons incidentally subjected to the surveillance;

(ii) train persons in the course of surveillances otherwise authorized by this title; or

(iii) train persons in the use of such equipment without engaging in electronic surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and

(C) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible.

(g) Certifications made by the Attorney General pursuant to section 102(a) and applications made and orders granted under this title shall be retained for a period of at least ten years from the date of the certification of application.

USE OF INFORMATION

SEC. 106. (a) Information acquired from an electronic surveillance conducted pursuant to this title concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this title. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this title shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this title may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) No information acquired pursuant to this title shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(c) Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this title, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

(d) Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this title, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(e) Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that—

(1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) Whenever a court or other authority is notified pursuant to subsection (c) or (d), or whenever a motion is made pursuant to subsection (e), or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this Act, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, rview in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved per-

son was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) If the United States district court pursuant to subsection (f) determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Orders granting motion or requests under subsection (g), decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

(i) In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

(j) If an emergency employment of electronic surveillance is authorized under section 105(e) and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of—

(1) the fact of the application;

(2) the period of the surveillance; and

(3) the fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

REPORT OF ELECTRONIC SURVEILLANCE

SEC. 107. In April of each year, the Attorney General shall transmit to the Administrative Office of the United States Courts and to Con-

gress a report setting forth with respect to the preceding calendar year—

(a) the total number of applications made for orders and extensions of orders approving electronic surveillance under this title; and

(b) the total number of such orders and extensions either granted, modified, or denied.

CONGRESSIONAL OVERSIGHT

SEC. 108. (a) On a semiannual basis the Attorney General shall fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence concerning all electronic surveillance under this title. Nothing in this title shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties.

(b) On or before one year after the effective date of this Act and on the same day each year for four years thereafter, the Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence shall report respectively to the House of Representatives and the Senate, concerning the implementation of this Act. Said reports shall include but not be limited to analysis and recommendations concerning whether this Act should be (1) amended, (2) repealed, or (3) permitted to continue in effect without amendment.

PENALTIES

SEC. 109. (a) OFFENSE.—A person is guilty of an offense if he intentionally—

(1) engages in electronic surveillance under color of law except as authorized by statute; or

(2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute.

(b) DEFENSE.—It is a defense to a prosecution under subsection (a) that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.

(c) PENALTY.—An offense described in this section is punishable by a fine of not more than $10,000 or imprisonment for not more than five years, or both.

(d) JURISDICTION.—There is Federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed.

CIVIL LIABILITY

SEC. 110. CIVIL ACTION.—An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 101(a) or

(b)(1)(A), respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 109 shall have a cause of action against any person who committed such violation and shall be entitled to recover—

(a) actual damages, but not less than liquidated damages of $1,000 or $100 per day for each day of violation, whichever is greater;

(b) punitive damages; and

(c) reasonable attorney's fees and other investigation and litigation costs reasonably incurred.

AUTHORIZATION DURING TIME OF WAR

SEC. 111. Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress.

TITLE II—CONFORMING AMENDMENTS

AMENDMENTS TO CHAPTER 119 OF TITLE 18, UNITED STATES CODE

SEC. 201. Chapter 119 of title 18, United States Code, is amended as follows:

(a) Section 2511(2)(a)(ii) is amended to read as follows:

"(ii) Notwithstanding any other law, communication common carriers, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire or oral communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if the common carrier, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with—

"(A) a court order directing such assistance signed by the authorizing judge, or

"(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No communication common carrier, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished an order or certification under this subparagraph, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal

prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any violation of this subparagraph by a communication common carrier or an officer, employee, or agent thereof, shall render the carrier liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any communication common carrier, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of an order or certification under this subparagraph.".

(b) Section 2511(2) is amended by adding at the end thereof ter" after "communication".

"(e) Notwithstanding any other provision of this title or section 605 or 606 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

"(f) Nothing contained in this chapter, or section 605 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications by a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted.".

(c) Section 2511(3) is repealed.

(d) Section 2518(1) is amended by inserting "under this chapter" after "communication".

(e) Section 2518(4) is amended by inserting "under this chapter" after both appearances of "wire or oral communication".

(f) Section 2518(9) is amended by striking out "intercepted" and inserting "intercepted pursuant to this chapter" after "communication".

(g) Section 2518(10) is amended by striking out "intercepted" and inserting "intercepted pursuant to this chapter" after the first appearance of "communication".

(h) Section 2519(3) is amended by inserting "pursuant to this chapter" after "wire or oral communications" and after "granted or denied".

TITLE III—EFFECTIVE DATE

EFFECTIVE DATE

SEC. 301. The provisions of this Act and the amendments made hereby shall become effective upon the date of enactment of this Act, except that any electronic surveillance approved by the Attorney General to gather foreign intelligence information shall not be deemed unlawful for failure to follow the procedures of this Act, if that sur-

veillance is terminated or an order approving that surveillance is obtained under title I of this Act within ninety days following the designation of the first judge pursuant to section 103 of this Act.

And the House agree to the same.

That the Senate recede from its disagreement to the amendment of the House to the title of the Senate bill and agree to the same.

And the House agree to the same.

EDWARD P. BOLAND,
MORGAN F. MURPHY,
R. L. MAZZOLI,
PETER W. RODINO,
ROBERT W. KASTENMEIER,
Managers on the Part of the House.

EDWARD M. KENNEDY,
JAMES ABOUREZK,
HOWARD M. METZENBAUM,
BIRCH BAYH,
JOE BIDEN,
ROBERT MORGAN,
BILL HATHAWAY,
STROM THURMOND,
JAKE GARN,
CHARLES MCC. MATHIAS, JR.,
Managers on the Part of the Senate.

JOINT EXPLANATORY STATEMENT OF THE COMMITTEE OF CONFERENCE

The managers on the part of the House and the Senate at the conference on the disagreeing votes of the two Houses on the amendments of the House to the bill (S. 1566) to amend title 18, United States Code, to authorize applications for a court order approving the use of electronic surveillance to obtain foreign intelligence information, submit the explanation of the effect of the action agreed upon by the managers and recommended in the accompanying conference report.

The managers recommend that the Senate agree to the amendments of the House, with an amendment. That amendment will be referred to here as the "conference substitute." Except for certain clarifying, clerical, conforming, and other technical changes, there follows an issue by issue summary of the Senate bill, the House amendments, and the conference substitute.

TITLE

The Senate bill amended Title 18 (Crimes and Criminal Procedures) of the United States Code, to authorize applications for a court order approving the use of electronic surveillance to obtain foreign intelligence information.

The House amendments provided for an uncodified title, to authorize electronic surveillance to obtain foreign intelligence information.

The conference substitute adopts the House provision. The conferees agree that this change is not intended to affect in any way the jurisdiction of Congressional Committees with respect to electronic surveillance for foreign intelligence purposes. Rather, the purpose of the change is solely to allow the placement of Title I of the Foreign Intelligence Surveillance Act in that portion of the United States Code (Title 50) which most directly relates to its subject matter.

DEFINITION OF "FOREIGN POWER"

The Senate bill defined "foreign power", with respect to terrorist groups, to mean a foreign-based terrorist group.

The House amendments defined "foreign power" to include a group engaged in international terrorism or activities in preparation therefor.

The conference substitute adopts the House definition. The conferees agree that the limitation to foreign-based groups may be unnecessarily burdensome and that surveillance of a group engaged in preparation for international terrorism may be necessary.

DEFINITION OF "AGENT OF A FOREIGN POWER"

The Senate bill defined "agent of a foreign power", with respect to persons other than U.S. persons, to include persons who act in the

United States as officers or employees of foreign powers; and certain persons who act for or on behalf of foreign powers which engage in clandestine intelligence activities contrary to the interests of the United States. With respect to any person, including a U.S. person, the Senate bill defined "agent of a foreign power" to include, *inter alia*, persons who knowingly engage in activities in furtherance of sabotage or terrorism for or on behalf of a foreign power; and persons who conspire with any person knowing that such person is engaged in specified activities.

The House amendments defined "agent of a foreign power", with respect to persons other than U.S. persons, to include persons who act in the United States as officers, *members*, or employees of foreign powers; and certain persons who act for or on behalf of foreign powers; which engage in clandestine intelligence activities in the United States contrary to the interests of the United States. With respect to any person, including a U.S. person, the House amendment defined "agent of a foreign power" to include, *inter alia*, persons who knowingly engage in activities that are in preparation for sabotage or international terrorism for or on behalf of a foreign power; and persons who knowingly conspire with any person to engage in specified activities.

The conference substitute adopts the House definition except that the definition with respect to persons other than U.S. persons includes members of groups engaged in international terrorist activities or activities in preparation therefor, rather than members of any foreign power. The conferees agree that surveillance of non-resident aliens who act as members of international terrorist groups may be necessary. The conferees note that a member of an international terrorist group will most likely not identify himself as such upon entering the United States, as would an officer or employee of a foreign power. In the latter instance, a copy of the person's visa application will usually suffice to show that he is acting in the United States as an officer or employee of a foreign power. However, in the case of a member of an international terrorist group, the government will most likely have to rely on more circumstantial evidence, such as concealment of one's true identity or affiliation with the group, or other facts and circumstances indicate that such person is in the United States for the purpose of furthering terrorist activities. The conferees also agree that the "preparation" standard for surveillance of U.S. persons does not mean preparation for a specific violent act, but for activities that involve violent acts. It may reasonable be interpreted to cover providing the personnel, training, funding or other means for the commission of acts of international terrorism. It also permits surveillance at some point before the dangers sought to be prevented actually occur. The remaining House provisions improve the clarity of the definition.

DEFINITION OF "INTERNATIONAL TERRORISM"

The Senate bill defined "terrorism" as activities which are violent acts or an act dangerous to human life which would be criminal under the laws of the United States or of any State if committed within its jurisdiction; and appear intended to achieve certain ends.

The House amendments defined "international terrorism" as activities that involve violent acts or acts dangerous to human life or property that are or may be a violation of the criminal laws of the United States or of any State, or that might involve a criminal violation if committed within the jurisdiction of the United States or any State. In addition to the apparent intent to achieve certain ends, the definition required that such acts occur totally outside the United States, or transcend national boundaries in certain ways.

The conference substitute adopts the House definition, modified to incorporate essentially the Senate criminal standard and to delete the words "or property." The conferees agree that the violent acts covered by the definition mean both violence to persons and grave or serious violence to property. The conferees also agree that surveillance of U.S. persons whose terrorist acts transcend national boundaries in certain ways may be necessary, but that the Senate criminal standard is more appropriate because domestic organizations may be included.

The conferees believe that the House standard "may be a violation" is redundant because the term "preparation" in the definitions of "foreign power" and "agent of a foreign power" permits surveillance at some point before the unlawful acts sought to be prevented actually occur, and because the definition of "agent of a foreign power" permits the surveillance of nonresident aliens who act in the United States as members of international terrorist groups regardless of whether or not such individuals may engage in unlawful acts.

DEFINITION OF "SABOTAGE"

The Senate bill defined "sabotage" as activities which would be prohibited by title 18, United States Code, chapter 105, if committed against the United States.

The House amendments defined "sabotage" as activities that involve or may involve a violation of chapter 105 of title 18, United States Code, or that might involve such a violation if committed against the United States.

The conference substitute defines "sabotage" as activities that involve a violation of chapter 105 of title 18, United States Code, or that would involve such a violation if committed against the United States. The conferees believe that the House term "may" is redundant because the term "preparation" in the definitions of "foreign power" and "agent of a foreign power" permits surveillance at some point before the violation actually occurs.

DEFINITION OF FOREIGN INTELLIGENCE INFORMATION

The Senate bill defined "foreign intelligence information," in part, as "information which relates to, and if concerning a United States person is necessary to, the ability of the United States to protect itself against" certain defined actions, and, as "information with respect to a foreign power or foreign territory which relates to, and if concerning a U.S. person is necessary to (i) the national defense or security of the nation; or (ii) the successful conduct of the foreign affairs of the United States."

The House amendments deleted the words "itself" and "successful". The conference substitute adopts the House version.

DEFINITION OF "ELECTRONIC SURVEILLANCE"

The Senate bill's inclusion of wire communications intercepted within the United States in the definition of "electronic surveillance" concluded with the words "while the communication is being transmitted by wire."

The House amendments omitted these words from the otherwise identical provision.

The conference substitute adopts the House definition because it conforms with the separate definition of "wire communication" in the House amendments and contained in the conference substitute.

DEFINITION OF "MINIMIZATION PROCEDURES"

The Senate bill defined "minimization procedures" as procedures which are reasonably designed to minimize the acquisition and retention, and prohibit the disseminaton, of any information concerning U.S. persons without their consent that does relate to specified interests; and to insure that national defense or foreign affairs information shall not be disseminated in a manner which identifies any United States person, without such person's consent, unless such person's identity is necessary to understand or assess the importance of information with respect to a foreign power or foreign territory or such information is otherwise publicly available. An exception cross-referenced later provisions allowing use of information that is evidence of a crime for law enforcement purposes.

The House amendments defined "minimization procedures", with respect to electronic surveillance, as specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition, retention, and dissemination of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information; and procedures that require that nonpublicly available national defense or foreign affairs information shall not be disseminated in a manner that identifies an individual United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance. A separate part of the definition allowed for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for the purpose of preventing the crime or enforcing the criminal law. In addition, the definition provided that the procedures, with respect to the warrantless surveillances authorized by section 102(a), require that no contents of any communication to which a U.S. person is a party shall be disclosed, disseminated, used, or retained for more than 24 hours unless a court order under section 105 is obtained.

The conference substitute adopts the House definition, with the following modifications. The procedures are to be reasonably designed

to minimize the acquisition and retention, and prohibit the dissemination, of specified information. The conferees agreed that the standard for dissemination should be higher than for acquisition and retention, but that the prohibition of dissemination should be reasonably designed to be consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. The procedures regarding the national defense or foreign affairs information apply to the identity of any United States person, rather than individends only. The conferees agree that the adjectival use of the name of a United States person entity, such as the brand name of a product, is not restricted by this provision because such information is publicly available. By "necessary" the conferees do not mean that the identity must be essential to understand the information or assess its importance. The word necessary requires that a knowledgeable intelligence analyst make a determination that the identity will contribute in a meaningful way to the ability of the recipient of the information to understand the information or assess its importance. The procedures also allow for the retention or dissemination of criminal evidence for law enforcement purposes. The conferees agree that such purposes include arrest, prosecution, and other law enforcement measures taken for the purpose of preventing the crime.

DEFINITION OF "UNITED STATES PERSON"

The Senate bill excluded corporations or associations from the definition of "United States person" if they also met any of the first five definitions of "foreign power."

The House amendments limited this exclusion to the first three definitions of foreign powers.

The conference substitute adopts the House version. The effect is to include international terrorist groups substantially composed of U.S. citizens or permanent resident aliens within the definition of "United States person." This does not in any way prohibit surveillance of such a group if it meets the definition of "foreign power." What it does is insure that the minimization procedures will apply to the surveillance of such a group, and that the intentional surveillance of the international communications of such a group in the United States, by intentionally targeting them, will require a court order and a judicial determination that the group is in fact a foreign power. (See section 101(f)(1) of the conference substitute.)

OTHER DEFINITIONS

The Senate bill included the Canal Zone within the definition of "United States," and adopted by cross-reference the definitions of "aggrieved person," "wire communication," "person," "contents," and "State" contained in Chapter 119 of Title 18, United States Code.

The House amendments deleted the Canal Zone from the definition of "United States," and adopted separate definitions of the other terms for the Foreign Intelligence Surveillance Act so as to conform to the provisions of the Act.

The conference substitute adopts the House definitions.

AUTHORITY TO APPROVE ELECTRONIC SURVEILLANCE

The House amendments contained a provision, not found in the Senate bill, which authorized, upon Attorney General certification, warrantless electronic surveillances directed at communications exclusively between or among "official" foreign powers, as defined in section 101(a)(1), (2), or (3), or directed at acquiring technical intelligence from property or premises under the open and exclusive control of such foreign powers. These surveillances were to be conducted under minimization procedures promulgated by the Attorney General which met the definition contained in section 101(h) and which were reported to the Intelligence Committees at least 30 days prior to their effective date. Section 101(h)(4) of the House amendments also stated that such procedures must require that no contents of any communication of a United States person acquired from a surveillance authorized by section 102(a) could be disclosed, disseminated, used, or retained for longer than 24 hours unless a court order was obtained.

The conference substitute adopts the House provision with the following modifications.

The authority for warrantless surveillance of communications of "official" foreign powers is modified to require that the surveillance be solely directed at the acquisition of the contents of communications transmitted by means of communication used exclusively between or among "official" foreign powers. This change excludes the targeting of lines or channels of communications that are used both by foreign powers and by other persons. This is intended to make entirely clear what was intended by the original House language.

A provision is added requiring the Attorney General to certify that there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party. This more accurately expresses the intent of the original House language.

Another requirement is added that the Attorney General assess compliance with the minimization procedures and report such assessments to the Intelligence Committees under the provisions of section 108(a). While the conferees did not retain the original House language of 108(b) requiring the intelligence committees to review all electronic surveillance, the conference substitute requires that the Attorney General report compliance with minimization procedures under section 102(a) to the committees so that they may assure themselves that minimization is properly conducted in this area where judicial review of minimization does not occur.

Finally, a provision is added to require the Attorney General immediately to transmit under seal to the court established under section 103(a) a copy of his certification. This provision also requires that such certification be maintained under security measures established by the Chief Justice with the concurrence of the Attorney General and remain sealed, unless an application for a court order with respect to the surveillance is made under section 101(h)(4) or the certification is necessary to determine the legality of the surveillance under section 106(f). This provision was added to provide appropriate executive branch accountability for these surveillances under the provisions of

section 102(a) consistent with the Senate preference for greater judicial involvement.

The conferees intend that both the Chief Justice and the Attorney General shall approve the security measure under which the sealed certifications are to be stored. Such measures may differ from those established under section 103(c) so as to take account of the greater sensitivity of the certifications. No court shall have jurisdiction to order that the sealed certification be unsealed for examination or review except in two circumstances: If an application for a court order with respect to the surveillance is made under section 101(h)(4), the judge to whom the application is made may examine the certification authorizing the surveillance. If a U.S. district court determines under the procedures of section 106(f) that the certification is necessary to determine the legality of the surveillance, the court may order that the certification be unsealed for review by the court. Such court order is final and binding, and therefore appealable by the Government, under section 106(h).

The conferees do not intend by this provision to authorize the Attorney General to direct electronic surveillance against a line or channel of communication substantially likely to carry conversations or messages of U.S. persons. The surveillance is not to be directed at any individual, even an agent of a foreign power. Instead, it may be directed only at "official" foreign powers themselves, that is, the communications of the foreign power or the property or premises of the foreign power. The Attorney General must certify that the surveillance is directed solely at communications of foreign powers, or at property or premises of foreign powers. He cannot make this certification if the surveillance is directed at an individual, or an agent of a foreign power, rather than at the foreign power itself. A court order is required for any surveillance that is directed at an individual, rather than at the communications, property, or premises of a foreign power.

The provision regarding communications "exclusively between or among" official foreign powers only empowers the Attorney General to authorize surveillances of those lines or channels of communications used by foreign powers exclusively to communicate among or between themselves. Since it is not foreseeable that U.S. persons would make use of such lines or channels of communications, the conferees have no reason to expect that the conversations or messages of U.S. persons will be subject to acquisition through a surveillance authorized under this susbection. Additional protection is provided by section 101(h)(4) which requires, in the highly unlikely event of such acquisition, that any communication of a U.S. person be destroyed within 24 hours unless its retention is authorized by a court order. The conferees do not intend that this provision permit the Attorney General to authorize the surveillance of a line or channel of communication substantially likely to be used by U.S. persons on the theory that the surveillance is to be limited to a period of time when such line or channel is used exclusively for communications among or between "official" foreign powers.

The conferees do not intend the term "technical intelligence" to include spoken communications of individuals. Thus a surveillance that is directed solely at the acquisition of technical intelligence from property or premises under the open and exclusive control of an

"official" foreign power does not include a surveillance intended to acquire spoken communications, whether or not passed telephonically. Further, the conferees intend that the acquisition of technical intelligence shall not include the use of a surveillance device for monitoring property or premises to observe individual United States persons.

Section 102(b) of the House amendments included language, not appearing in the Senate bill, that authorized the approval of electronic surveillance applications "notwithstanding any other law."

The conference substitute adopts the House version. The words "notwithstanding any other law" are intended to make it clear that electronic surveillance may be approved notwithstanding any other statute, such as section 1251 of title 28, United States Code, which grants the Supreme Court exclusive original jurisdiction over all actions against ambassadors of foreign states, or any treaty or international agreement.

DESIGNATION OF JUDGES

The Senate bill provided that the Chief Justice should publicly designate seven district judges constituting a special court with jurisdiction to hear applications for and grant orders approving electrontic surveillance anywhere within the United States; and three additional judges from the United States district courts or courts of appeals to comprise a special court of review with jurisdiction to review the denial of application. Provisions were also made for written statements of reasons for decisions denying applications and for Supreme Court review of decisions of the court of review denying applications. Proceedings were to be conducted as expeditiously as possible, and the record of proceedings was to be sealed and maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of Central Intelligence. The designated judges were to serve staggered, 7-year terms, and were not eligible for redesignation.

The House amendments provided that the U.S. district courts should have jurisdiction to receive application and issue orders for electronic surveillance. Proceedings were to be conducted as expeditiously as possible. If an application was denied, the court was to record the reasons for that denial and, upon the motion of the applicant, such reasons were to be transmitted under seal to the U.S. court of appeals.

The conference substitute adopts a compromise provision which grants nationwide jurisdiction to a court composed of seven judges publicly designated by the Chief Justice from seven different judicial circuits, who will exercise the jurisdiction granted to the court under this Act. Further, the Chief Justice shall designate three judges from the judges of the United States district courts or courts of appeals who shall constitute a court of review.

The conferees intend that the court shall sit continuously in the District of Columbia, that the designated judges shall serve by rotation determined by the Chief Justice, that they may be assigned to other judicial duties in the District of Columbia which are not inconsistent with their duties under this Act, and that more than one judge shall be available at all times to perform the duties required by this

Act. The conferees expect that the Chief Justice will consult with the chief judges of the judicial circuits in making designations of judges under this section.

The conference substitute is otherwise the same as the Senate provision, except that the requirement for sealing records is deleted. The conferees agree that the designated judges should have an opportunity to examine, when appropriate, the applications, orders, and statements of reasons for decisions in other cases. The conferees also agree that the security measures to be established by the Chief Justice shall include such document, physical, personnel, or communications security measures as are necessary to protect information concerning proceedings under this Act from unauthorized disclosure. Such measures may also include the use of secure premises provided by the executive branch to hear an application and the employment of executive branch personnel to provide clerical and administrative assistance.

CONTENTS OF APPLICATION

The Senate bill required that the application state the facilities or place at which the surveillance is directed and whether physical entry is required. If the target is an "official" foreign power the Senate bill required no detailed statement of the nature of the information sought, but only a designation of the type of information according to the categories of the definition of "foreign intelligence information"; and no statement of the means of surveillance, except for a designation of the type of electronic surveillance according to the categories of the definition and whether physical entry is required.

The House amendments required the application to state "each of" the facilities or places at which the surveillance is directed, but not whether physical entry is required. The House amendments also required a statement, not contained in the Senate bill, of the coverage and minimization procedures applying to each device whenever multiple devices are used. If the target is an "official" foreign power, the House amendments required that the application contain such information about the surveillance techniques and communications or other information concerning United States persons likely to be obtained as may be necessary to assess the proposed minimization procedures.

The conference substitute adopts the House provisions requiring the application to state "each of" the facilities and the coverage and minimization procedures where multiple devices are used. It is contemplated that separate minimization procedures will be required for each device only where the placement or coverage of each device raises separate privacy considerations. The conference substitute adopts the Senate requirement that the application state whether physical entry is required. The conferees agree that physical entry may be authorized to effect electronic surveillance under this bill.

The conference substitute also adopts the provision of the House amendments requiring, in the case of "official" foreign powers, that the application contain information about the surveillance techniques and communications or other information concerning United States persons likely to be obtained as may be necessary to assess the proposed minimization procedures.

CONTENTS OF CERTIFICATION

The Senate bill required a certification by the Assistant to the President for National Security Affairs *or* an executive branch official appointed by the President with the advice and consent of the Senate. The certification was to include a statement of the duration of surveillance of an "official" foreign power.

The House amendments required a certification by the Assistant to the President for National Security Affairs and an executive branch official appointed by the President with the advice and consent of the Senate. The certification would not include a statement of the duration of surveillance of an "official" foreign power.

The conference adopts the Senate provision regarding certification by the Assistant to the President, and deletes from the certification the statement of duration of surveillance of an "official" foreign power. The conferees agree that the Director of the Federal Bureau of Investigation, who is appointed by the President with the advice and consent of the Senate, should not have to secure a certification from a White House official before obtaining the Attorney General's approval. Such a procedure could result in harmful delay in an emergency situation. The conferees also agree that the application itself is sufficient for the statement of duration.

JUDICIAL FINDINGS

Both the Senate bill and the House amendments contained a proviso insuring that protected First Amendment activities could not be the sole basis for approving a surveillance targeted against a United States person.

The Senate bill placed this proviso in the definition of "agent of a foreign power." The House amendments placed it in section 105(a), dealing with judicial findings, and extended its coverage to "foreign powers" as well as "agents of a foreign power" because groups composed substantially of U.S. persons can be considered foreign powers. The House version has been adopted.

CONTENTS OF ORDER

The Senate bill contained provisions generally paralleling its requirements for the contents of an application, including whether physical entry will be required, and a provision permitting the judge to direct a communications carrier or other person to provide all information, facilities, or technical assistance necessary to accomplish the electronic surveillance "in such a manner as will protect its secrecy."

The House amendments contained provisions generally paralleling their requirements for the contents of an application, and a similar provision regarding assistance which required that it be furnished "unobtrusively and in such a manner as will protect its secrecy."

The conference substitute adopts the House provisions generally paralleling the requirements for the contents of an application, the Senate provision regarding physical entry, and the Senate provision regarding assistance which omits the words "unobtrusively and." The conferees note that this is a change in wording from a similar provision in chapter 119 of title 18, United States Code. The change is in

tended to emphasize the increased sensitivity of the surveillances conducted under the Foreign Intelligence Surveillance Act and the corresponding need to maintain secrecy. However, the nature and scope of such assistance is intended to be identical to that which may be directed under section 2518(4)(e) of chapter 119.

EXTENSIONS

The Senate bill required 90-day extensions for all surveillances, except for 1-year surveillances of "official" foreign powers. It provided that the judge may require the applicant to submit information, obtained pursuant to the original order or any previous extensions, as may be necessary to make new findings of probable cause. The Senate bill also provided that the judge may assess compliance with the minimization procedures.

The House amendments required 90-day extensions for all surveillances, except for 1-year surveillances of "official" foreign powers and 1-year extensions for the other categories of foreign power if the judge found probable cause to believe that no communication of any individual U.S. person would be acquired during the period. The House amendments included no provision specifically allowing the judge to require submission of previously obtained information. The House amendments also provided that, at the end of the period of time for which electronic surveillance was approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

The conference substitute adopts the House provisions, with the following modifications. One-year extensions are not authorized for the international terrorist group category of foreign powers, if the group is a United States person. In addition, the judge may assess compliance with the minimization procedures at or before the end of the period of time for which electronic surveillance is approved by an order or an extension.

Finally, the conferees believe that the Senate provision allowing the judge to require submission of previously obtained information is redundant, in view of the authority already granted to the judge in section 104(d) to require the applicant to furnish such other information as may be necessary to make the determinations required for granting an extension.

EMERGENCY SURVEILLANCE

The Senate bill prohibited any use of information concerning United States persons that might be acquired from an emergency surveillance that a judge did not subsequently approve, except where the information indicates a threat of death or serious bodily harm to any person.

The House amendments contained a comparable provision, with an exception if the information may indicate a threat of death or serious bodily harm to any person.

The conference substitute adopts the Senate provision which omits the word "may." The conferees agree that an exception for any indication of such a threat is sufficient.

TESTING, DETECTION, AND TRAINING AUTHORITY

The Senate bill provided authority for the testing of electronic surveillance equipment and the detection of unlawful electronic surveillance. The testing provision required the approval of the Attorney General for tests extending beyond a period of 90 days.

The House amendments provided comparable testing and detection authority, with the addition of certain safeguards but deletion of the requirement of Attorney General approval for tests extending beyond 90 days. The House amendments also added a provision, not contained in the Senate bill, to provide authority for the training of personnel when such testing as may be authorized by the Attorney General does not provide sufficient opportunities for training.

The conference substitute adopts the House provisions, with the addition of the Senate requirement of approval of the Attorney General for tests exceeding 90 days. The conferees agree that this requirement shall result in Attorney General approval of testing which extends or will extend beyond a period of 90 days. The approval shall be for specified periods of time; and if these periods are exceeded, new approval shall be sought.

RECORDS RETENTION

The House amendments included a provision, not contained in the Senate bill, that certifications of the Attorney General and applications and orders shall be retained for a period of 10 years and stored at the direction of the Attorney General under security procedures approved by the Director of Central Intelligence.

The conference substitute retains the provision for 10 year retention for oversight purposes, but does not require that storage be at the direction of the Attorney General because such document security measures as are appropriate under section 103(c) for applications and orders will be established by the Chief Justice in consultation with the Attorney General and the Director of Central Intelligence. Storage of certifications made under section 102(a) will be at the direction of the Attorney General except as otherwise provided in section 102(a)(3).

AUTHORITY TO USE INFORMATION

The Senate bill authorized use and disclosure of information concerning U.S. persons only for purposes specified in the definition of "minimization procedures" and in accordance with the minimization procedures, or for the enforcement of the criminal law if its use outweighs the possible harm to the national security.

The House amendments authorized use and disclosure of information concerning United States persons only in accordance with the minimization procedures.

The conference substitute adopts the House provisions. The conferees agree that these provisions are appropriate in view of the definition of "minimization procedures" in the conference substitute. The conferees believe that, even without a statutory requirement, there will be an appropriate weighing of criminal law enforcement needs against possible harm to the national security.

NOTICE OF USE OF INFORMATION IN LEGAL PROCEEDINGS

The Senate bill provided for notification to the court when information derived from electronic surveillance is to be used in legal proceedings.

The House amendments contained a comparable provision and also a provision, not contained in the Senate bill, requiring notice to the aggrieved person. The House amendments also contained a separate section relating to use by State or local authorities requiring notice to the Attorney General.

The conference substitute adopts the House provisions. The conferees agree that notice should be given to the aggrieved person as soon as possible, so as to allow for the disposition of any motions concerning evidence derived from electronic surveillance. The conferees also agree that the Attorney General should at all times be able to assess whether and to what extent the use of information made available by the Government to a State or local authority will be used.

SUPPRESSION MOTIONS

The Senate bill provided for motions to suppress the contents of any communication acquired by electronic surveillance, or evidence derived therefrom.

The House amendments provided for motions to suppress the evidence obtained or derived from electronic surveillance.

The conference substitute adopts the House provision. The conferees agree that the broader term "evidence" should be used because it includes both the contents of communications and other information obtained or derived from electronic surveillance.

IN CAMERA PROCEDURE FOR DETERMINING LEGALITY

The Senate bill provided a single procedure for determining the legality of electronic surveillance in a subsequent in camera and ex parte proceeding, if the Government by affidavit asserts that disclosure or an adversary hearing would harm the national security of the United States. The Senate bill also provided that, in making this determination, the court should disclose to the aggrieved person materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

The House amendments provided two separate procedures for determining the legality of electronic surveillance, if the Attorney General files an affidavit under oath that disclosure would harm the national security of the United States or compromise foreign intelligence sources and methods. In criminal cases, there would be an in camera proceeding; and the court might disclose to the aggrieved person, under appropriate security procedures and protective orders, materials relating to the surveillance if there were a reasonable question as to the legality of the suveillance and if disclosure would likely promote a more accurate determination of such legality, or if disclosure would not harm the national security. In civil suits, there would be an in camera and ex parte proceeding before a court of appeals; and the court would disclose, under appropriate security procedures and protective orders, to the aggrieved person or his attorney materials relat-

ing to the surveillance only if necessary to afford due process to the aggrieved person. The House amendments also provided that orders regarding legality or disclosure would be final and binding.

The conference substitute essentially adopts the Senate provisions, with technical changes and the following modifications. The in camera and ex parte proceeding is invoked if the Attorney General files an affidavit under oath. All orders regarding legality and disclosure shall be final and binding only where the rulings are against the Government.

The conference substitute adds the words "requiring review or" to the provision making orders final and binding. This change clarifies the intent of the House provision in conformity with section 102(a). The conferees intend that a determination by a district court that review of a certification by the Attorney General under section 102(a) is necessary to determine the legality of the surveillance shall be considered a final and binding order and thus appealable by the Government before the court reviews the certification. The court may order that the certification be unsealed for review if such review is necessary to determine the legality of the surveillance.

The conferees agree that an in camera and ex parte proceeding is appropriate for determining the lawfulness of electronic surveillance in both criminal and civil cases. The conferees also agree that the standard for disclosure in the Senate bill adequately protects the rights of the aggrieved person, and that the provision for security measures and protective orders ensures adequate protection of national security interests.

UNITENTIONAL RADIO ACQUISITION

The Senate bill prohibited any use of the contents of unintentionally acquired domestic radio communications, if there is a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, except where the contents indicate a threat of death or serious bodily harm to any person.

The House amendments contained a comparable provision, with an exception if the contents may indicate a threat of death or serious bodily harm to any person.

The conference substitute adopts the Senate provision which omits the word "may." The conferees agree that an exception for any indication of such a threat is sufficient.

CONGRESSIONAL OVERSIGHT

The Senate bill and the House amendments both require the Attorney General, on a semiannual basis, to fully inform the intelligence committees of each House concerning all electronic surveillance under the act.

The Senate bill also stated that "nothing in this chapter shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties."

The House amendments limited this reservation to the respective intelligence committees. The conference substitute adopts the Senate version.

Section 2528(b) of the Senate bill required the Senate Intelligence Committee to report annually to the Senate on the implementation of

the act, with recommendations as to whether it should be amended or repealed. The House amendments contained no similar provision.

Section 108(b) of the House amendments required the respective intelligence committees when, through review of the information provided by the Attorney General, they determined that a surveillance of a U.S. person produced no foreign intelligence information and the national security would not be harmed, to notify the target of such surveillance.

The conference substitute adopts a modified version of the Senate provision, requiring an annual review for only five years, and deletes the House provision.

Pursuant to the resolutions establishing each, both the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, currently possess the authority granted in the deleted House provision. However, it may be appropriate to further delineate the authority in separate legislation. The conferees expect that the annual reviews to be conducted by the respective intelligence committees will fully examine this issue.

CRIMINAL PENALTIES

The Senate bill provided, by conforming amendment to title 18, United States Code, for criminal penalties for any person who, under color of law, willfully engages in electronic surveillance except as provided in this bill; for any person who willfully discloses, or endeavors to disclose, to any other person information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through unlawful electronic surveillance; and for any person who willfully uses, or endeavors to use, information obtained through unlawful electronic surveillance.

The House amendments provided for separate criminal penalties in this act, rather than by conforming amendment to title 18, for any person who intentionally engages in electronic surveillance under color of law except as authorized by statute. A defense was provided for a defendant who was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.

The conference substitute adopts the House provision modified to add the Senate criminal penalty for any person who discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute. The conferees agree that the criminal penalties for intelligence agents under this Act should be essentially the same as for law enforcement officers under title 18.

CIVIL LIABILITY

The Senate bill provided, by conforming amendment to title 18, United States Code, that any person other than a foreign power or an agent of a foreign power (as defined with respect to officers or employees of foreign powers and certain other nonresident aliens) who has been subject to electronic surveillance, or about whom information has been disclosed or used, in violation of the criminal penalty pro-

visions, should have a civil cause of action against any person who so acted.

The House amendments provided for separate civil liability under this act, rather than by conforming amendment to title 18. Any person other than a foreign power or an agent of a foreign power (as defined with respect to officers, members, or employees of a foreign power) who has been subjected to an electronic surveillance or whose communication has been disseminated or used in violation of the criminal penalty provisions was granted a cause of action against any person who committed such violation.

The conference substitute adopts the House provision, modified to grant a cause of action to any aggrieved person about whom information has been disclosed or used in violation of the criminal penalty provisions. The conferees agree that the civil liability of intelligence agents under this act should coincide with the criminal liability. The conferees also agree that the House provisions regarding suits by certain nonresident aliens would have the same practical effect as the Senate provision.

AUTHORIZATION DURING TIME OF WAR

The House amendments contained a provision which would allow the President to authorize electronic surveillance for periods up to a year during time of war declared by Congress. The Senate bill had no comparable provision.

The conference substitute retains the House language but adds the further requirement that the Attorney General inform the intelligence committees of the facts and circumstances giving rise to the need for such authority, the scope of such authority, and the standards to be employed in exercising such authority.

The conference substitute adopts a compromise provision authorizing the President, through the Attorney General, to authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for a period not to exceed 15 calendar days following a declaration of war by the Congress.

The conferees intend that this period will allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency. The conferees also intend that all other provisions of this act not pertaining to the court order requirement shall remain in effect during this period. The conferees expect that such amendment would be reported with recommendations within 7 days and that each House would vote on the amendment within 7 days thereafter.

CONFORMING AMENDMENTS

The Senate bill contained certain conforming amendments to existing law, including a provision regarding assistance by common carriers in the conduct of electronic surveillance that imposed civil liability for violations.

The House amendments deleted several of the conforming amendments, and expanded the class of persons who are covered by the provision regarding assistance in the conduct of electronic surveillance under this bill and chapter 119 of title 18, United States Code, to include "landlords, custodians, and other persons." This provision pro-

vided for notice to the Attorney General or other appropriate official when or if any person who is ordered to provide assistance to the Government in conducting electronic surveillance is required by legal process to disclose the fact of such assistance. It also afforded civil immunity to any person who provides such assistance in accordance with a court order or Attorney General certificate.

The conference substitute adopts the House provisions, with the addition of the Senate provision imposing civil liability upon a common carrier which provides assistance without a court order or Attorney General certificate. Deletion of certain conforming amendments is consistent with the decision of the conferees not to place the bill in title 18, United States Code.

EXCLUSIVE MEANS FOR ELECTRONIC SURVEILLANCE

The Senate bill provided that the procedures in this bill and in chapter 119 of title 18, United States Code, shall be the exclusive means by which electronic surveillance, as defined in this bill, and the interception of domestic wire and oral communications may be conducted.

The House amendments provided that the procedures in this bill and in chapter 119 of title 18, United States Code, shall be the exclusive statutory means by which electronic surveillance as defined in this bill and the interception of domestic wire and oral communications may be conducted.

The conference substitute adopts the Senate provision which omits the word "statutory." The conferees agree that the establishment by this act of exclusive means by which the President may conduct electronic surveillance does not foreclose a different decision by the Supreme Court. The intent of the conferees is to apply the standard set forth in Justice Jackson's concurring opinion in the Steel Seizure Case: "When a President takes measures incompatible with the express or implied will of Congress, his power is at the lowest ebb, for then he can rely only upon his own Constitutional power minus any Constitutional power of Congress over the matter." *Youngstown Sheet and Tube Co.* v. *Sawyer*, 343 U.S. 579, 637 (1952).

EDWARD P. BOLAND,
MORGAN F. MURPHY,
R. L. MAZZOLI,
PETER W. RODINO,
ROBERT W. KASTENMEIER,
Managers on the Part of the House.

EDWARD M. KENNEDY,
JAMES ABOUREZK,
HOWARD M. METZENBAUM,
BIRCH BAYH,
JOE BIDEN,
ROBERT MORGAN,
BILL HATHAWAY,
STROM THURMOND,
JAKE GARN,
CHARLES MCC. MATHIAS, JR.,
Managers on the Part of the Senate.